

### **REMARKS**

Claims 1-10 are currently pending in the present application. Favorable reconsideration and allowance of the present application are respectfully requested in view of the following remarks.

#### **Claim Rejections Under 35 U.S.C. § 102**

Claims 1-10 are rejected under 35U.S.C. § 102(e) as being anticipated by Edgett et al. (U.S. Patent Publication No. US 2004/0034771) ("Edgett"). This rejection is respectfully traversed.

For a Section 102 rejection to be proper, the cited reference must teach or suggest each and every claimed element. See M.P.E.P. 2131; M.P.E.P. 706.02. Thus, if the cited reference fails to teach or suggest one or more elements, then the rejection is improper and must be withdrawn.

#### **Independent claim 1**

Independent claim 1 is directed to an authenticated device. The authenticated device includes, *inter alia*, "a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device; a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit."

The Examiner maintains that Edgett, in paragraphs [0057]-[0059], discloses the above-noted features. Applicants respectfully disagree.

In a response to Applicants' arguments in the previously filed response, the Examiner states that Edgett discloses updating the algorithm by changing the key pair. As such, Edgett discloses providing a key index and an algorithm identifier. First, Edgett is not directed to updating the algorithm by changing the key pair. Instead, Edgett merely discloses updating an algorithm or updating a key pair. See paragraphs [0051] and [0056]. Furthermore, while Applicants do not disagree with the assertion that Edgett discloses a key index and an algorithm

identifier, they are NOT a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit as claimed.

In contrast, Edgett merely discloses a method of updating an algorithm. Specifically, when a dialer containing an old algorithm communicates with a network, the dialer encrypts a password using the old algorithm. The encrypted password, a corresponding key index and an associated algorithm identifier are then transmitted to the server. The server then utilizes the algorithm identifier to identify the corresponding algorithm to be used for decrypting the password for authentication. Once the dialer is connected to the server, the dialer contacts the Update Server to determine if an algorithm update is required. If so, the new algorithm and its associated key identifier are downloaded to the dialer. See paragraphs [0056]-[0059] of Edgett. In other words, the dialer transmits old algorithm to the server for authentication and receives a new algorithm if there is an algorithm update required. However, the new algorithm and the new corresponding algorithm identifier represent an improved algorithm that has been developed and are completely unrelated to the old algorithm and the old corresponding algorithm identifier transmitted by the dialer. See paragraph [0057]. Thus, the new algorithm identifier of Edgett is NOT a prescribed algorithm identifier selected from among the at least one algorithm identifier transmitted as claimed. Therefore, Edgett does not disclose or suggest “a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device; a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit” as claimed.

#### Independent claim 4

Independent 4 is directed to an authenticating device. The authenticating device includes, *inter alia*, “a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one

algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit; a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device.”

The Examiner fails to respond to Applicants’ arguments in the previously filed response with respect to claim 4. It appears that the Examiner is maintaining that Edgett discloses the above-noted features. Applicants respectfully disagree.

Edgett discloses that a customization tool may store a private key, its corresponding key index and the algorithm identifier in a private key database of a server. However, Edgett is completely silent with respect to a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit as claimed. Specifically, the private key, its corresponding key index and the algorithm identifier stored by the customization tool are NOT a prescribed algorithm identifier and a prescribed encryption key identifier selected to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit as claimed.

Furthermore, even if, *arguendo*, the algorithm identifier stored by the customization tool in Edgett is the prescribed algorithm identifier selected from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, Edgett still fails to disclose or suggest a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device as claimed. The algorithm identifier stored by the customization tool in Edgett is not transmitted. Instead, Edgett discloses that when there is an algorithm update required, the new algorithm and corresponding algorithm identifier are downloaded to the dialer. The new algorithm and corresponding algorithm identifier represent an improved algorithm that has been developed and are completely unrelated to the algorithm identifier stored in the server by the customization tool. Thus, Edgett does not disclose or suggest “a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among

the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit; a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device” as claimed.

Independent claim 7

Independent claim 7 recites, *inter alia*, “a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step; a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device; a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device”.

The Examiner fails to respond to Applicants’ arguments in the previously filed response with respect to claim 7. It appears that the Examiner is maintaining that Edgett discloses the above-noted features. Applicants respectfully disagree.

It is demonstrated above that Edgett fails to teach or suggest the above-noted features for the reasons discussed with respect to claims 1 and 4.

Furthermore, Edgett is merely concerned with a dialup computer, which sends encrypted user credential to a server for gaining access to a network. If there is an updated key/algorithm, the server then sends the updated key/algorithm to the dialup computer. Therefore, a single set of key/algorithm is being communicated between the dialup computer and the server. Thus, Edgett does not teach or suggest “a first transmitting step to transmit, from an authenticated

device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored; a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier” as recited in claim 7.

Independent claim 8

Independent claim 8 recites, *inter alia*, “a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device by the first transmitting step, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers; a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step; a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device; a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device”.

The Examiner fails to respond to Applicants’ arguments in the previously filed response with respect to claim 8. It appears that the Examiner is maintaining that Edgett discloses the above-noted features. Applicants respectfully disagree.

It is demonstrated above that Edgett fails to teach or suggest the above-noted features for the reasons discussed with respect to claims 1, 4 and 7.

Independent claim 9

Independent claim 9 recites, *inter alia*, “transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored; receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier; selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received; transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device; receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device”.

The Examiner fails to respond to Applicants’ arguments in the previously filed response with respect to claim 9. It appears that the Examiner is maintaining that Edgett discloses the above-noted features. Applicants respectfully disagree.

It is demonstrated above that Edgett fails to teach or suggest the recited features for the reasons discussed with respect to claims 1, 4 and 7.

Independent claim 10

Independent claim 10 recites, *inter alia*, “transmitting, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored; receiving the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers; selecting, at the

authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received; transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device; receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device”.

The Examiner fails to respond to Applicants’ arguments in the previously filed response with respect to claim 10. It appears that the Examiner is maintaining that Edgett discloses the above-noted features. Applicants respectfully disagree.

It is demonstrated above that Edgett fails to teach or suggest the recited features for the reasons discussed with respect to claims 1, 4 and 7.

In view of the above remarks, it is respectfully submitted that Edgett does not anticipate independent claims 1, 4 and 7-10. As claims 2, 3, 5 and 6 are dependent to claims 1 and 4, respectively, it is respectfully submitted that these claims are also patentable for at least the same reasons discussed with respect to claims 1 and 4. Thus, it is respectfully submitted that these rejections should be withdrawn.

### **CONCLUSION**

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Dennis P. Chen Reg. No. 61,767 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

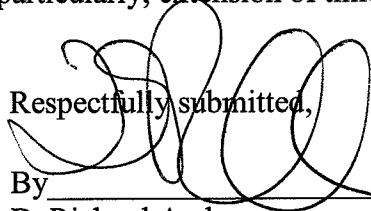
Application No. 10/584,194  
Amendment dated June 2, 2009  
After Final Office Action of April 3, 2009

Docket No.: 2565-0297PUS1

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: June 2, 2009

Respectfully submitted,



By \_\_\_\_\_

D. Richard Anderson

Registration No.: 40,439

BIRCH, STEWART, KOLASCH & BIRCH, LLP

8110 Gatehouse Road

Suite 100 East

P.O. Box 747

Falls Church, Virginia 22040-0747

(703) 205-8000

Attorney for Applicant